REMARKS

Initially, in the Office Action dated June 28, 2005, the Examiner objects to the Abstract because of informalities. Claims 1-12 have been objected to because of informalities. Claim 12 has been rejected under 35 U.S.C. §101. Claims 1-12 have been rejected under 35 U.S.C. §112, second paragraph. Claims 1-8, 11 and 12 have been rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,078,953 (Vaid et al.) in view of U.S. Patent No. 5,999,979 (Vellanki et al.) and further in view of U.S. Patent No. 6,029,164 (Birrell et al.). Claim 9 has been rejected under 35 U.S.C. §103(a) as being unpatentable over Vaid et al., Birrell et al. and Vellanki et al. and further in view of U.S. Patent Publication No. 2003/0033418 (Young et al.). Claim 10 has been rejected under 35 U.S.C. §103(a) as being unpatentable over the combination of Vaid et al., Birrell et al. and Vellanki et al. and further in view of U.S. Patent No. 5,996,025 (Day et al.).

By the present response, Applicants have submitted new claim 13 for consideration by the Examiner and submit that this claim does not contain any prohibited new matter. Further, Applicants have amended claims 1, 2 and 4-12 to further clarify the invention. Claims 1-13 remain pending in the present application.

Specification Objections

The Examiner has objected to the Abstract of the Disclosure. Applicants have submitted a new abstract that addresses the Examiner's concerns and respectfully request that this objection be withdrawn.

Claim Objections

Claims 1-12 have been objected to because of informalities. Applicants have amended the claims of the present application to further clarify the invention and respectfully request that these objections be withdrawn.

35 U.S.C. §101 Rejections

Claim 12 has been rejected under 35 U.S.C. §101. Applicants have amended this claim to further clarify the invention and respectfully request that this rejection be withdrawn.

35 U.S.C. §112 Rejections

Claims 1-12 have been rejected under 35 U.S.C. §112, second paragraph. Applicants have amended these claims to further clarify the invention and respectfully request that these rejections be withdrawn.

35 U.S.C. §103 Rejections

Claims 1-8, 11 and 12 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Vaid et al. in view of Vellanki et al. and further in view of Birrell et al. Applicants respectfully traverse these rejections.

Vaid et al. discloses a method and system for controlling quality of service within a network of computers where the method includes providing a network of computers, each being coupled to each other to form a local area network. The network of computers has a firewall server coupled to the network of computers and a traffic management tool coupled to the firewall server. The method also includes

12

implementing traffic control for incoming and outgoing information using a combination of flow control and queuing techniques.

Vellanki et al. discloses a method in a computer network for automatically detecting a most advantageous protocol for communication by a client computer, the client computer being configured to be coupled to a server computer via a computer network. The method includes initiating a plurality of protocol threads for sending from the client computer to the server computer, a plurality of data requests. Each of the data requests employs a different protocol and a different connection. The data requests are configured to solicit, responsive to the data request, a set of responses from the server computer. Each of the responses employs a protocol associated with a respective one of the data requests.

Birrell et al. discloses in a computer method for labeling data records, data records being received in an index server. The records are parsed into words, and the words are stored in a full-text index. Labels are added to the data records and the full-text index. The data records are accessed by searching the full-text index using queries including the words and the labels of the data records. Labels can be removed from the full-text index.

Regarding claims 1, 11, 12 and new claim 13, Applicants submit that none of the cited references, taken alone or in any proper combination, disclose, suggest or render obvious the limitations in the combination of each of these claims of, inter alia, a stream server apparatus that includes a first interface which transmits and receives packets to and from a relevant one (or first) of the client apparatuses

belonging to a first network without passing through the firewall apparatus, and transmits and receives packets to and from another relevant one (or second) of the client apparatuses belonging to a second network, different from a first network, via the firewall apparatus and the second network and without passing through the first network, or a second interface which transmits and receives packets to and from the another relevant one client apparatus belonging to a third network, different from the first network, via the third network and without passing through the firewall apparatus or the first network, the second interface being connected to a wide area network, or a stream transport management module which specifies the first interface or the second interface in accordance with a network attribute and a type of a communication protocol of one of the relevant one client apparatus or the another relevant one client apparatus, or where the process module executes a stream data distribution process based on a user datagram protocol (UDP) as the same communication protocol both for the first and second client apparatuses. The Examiner asserts that Vaid et al. discloses a first interface which transmits and receives a packet to and from the client apparatus belonging to a network different from the particular network via the firewall apparatus at col. 6, lines 18-25 and Fig. 1, connection between elements 120 and 220. However, these portions of Vaid et al. merely disclose that computers such as computers 130 and 140 and 210 communicate using any one of multiple application layer protocols and that communication across WAN 170 and across network connection 190 implements transport layer protocols such as TCP, UDP, etc., and Fig. 1 showing a connection

14

between file server 120 and computer 220 through firewall server 110 and the internet 200. However, this is not a first interface which transmits and receives packets to and from another relevant one (or second) of the client apparatuses belonging to a second network, different from a first network, via the firewall apparatus and the second network and without passing through the first network, as recited in the claims of the present invention.

Moreover, the Examiner admits that Vaid et al. does not disclose or suggest a first interface transmitting and receiving a packet to and from the client apparatus without the firewall apparatus, but asserts that Vaid et al. discloses these limitations with the connection between server 120 and in client 130. However, these portions of Vaid et al. are not a first interface which transmits and receives packets to and from a relevant one of the client apparatuses belonging to the first network without passing through the firewall apparatus and transmits and receives packets to and from another relevant one of the client apparatuses via a second network, different from the first network, via the firewall apparatus and without passing through the first network, as recited in the claims of the present application. Initially, nowhere in Vaid et al. is it disclosed that server 120 is a stream server apparatus, as recited in the claims of the present application. Further, server 120 is connected to desktop 220 via LAN 160 and is also connected to desktop computer 130 through the same LAN 160. In contrast, the limitations in the claims of the present application relate to a first interface that transmits and receives packets to and from another relevant one of the client apparatus belonging to a second network, different from the first

15

network, via the firewall apparatus and the second network and without passing through the first network. Vaid et al. discloses server 120 being connected via LAN 160 to desktop 130 and via LAN 160 to desktop 220.

The Examiner then asserts that Birrell et al. teaches that a firewall is used to provide security protection by filtering communication between the Internet and the intranet at col. 3, lines 54-62. Applicants are confused as to the relevance of this assertion by the Examiner. These portions of Birrell et al. merely disclose that the purpose of a firewall is to enforce security policies of the private intranet and protect accesses to critical resources (servers and data) of the intranet. This is merely a definition of a firewall which is known. Birrell et al. relates to organizing and accessing electronic mail messages using labels and full text and label indexing and has absolutely nothing to do with the technology as recited in the claims of the present application that relate to a stream server apparatus connected to client apparatuses and a firewall apparatus for inhibiting a packet from illegally accessing a first network. Birrell et al. does not disclose or suggest a stream server apparatus distributing stream data to the client apparatuses and including a first interface and a second interface, a stream transport management module, and a process module, as detailed in the claims of the present application.

Moreover, the Examiner admits that Vaid et al. fails to disclose or suggest a second interface which transmits and receives a packet to and from the client apparatus . . . as recited in the claims of the present application, but asserts that Vellanki et al. discloses these limitations at col. 2, lines 31-46, col. 13, lines 4-26,

16

and col. 9, line 52 – col. 10, line 3. However, these portions of Vellanki et al. merely disclose that certain types of data and/or protocols may be prevented from traversing through a firewall, and that a proxy may be used to allow a client application to communicate with a server in networks where it is not possible to traverse the firewall such as when a protocol is strictly prohibited by the firewall, that multiple protocols that may be employed for communication between a server computer and a client computer may be tried in parallel over different control connections by the client computer, and details of Fig. 4 describing a firewall being disposed between a client application and a server and the process of the client application sending control requests using a given protocol via the firewall to the server and the server responding with data via the data connection and via the firewall. Vellanki et al. merely relates to detecting the most advantageous protocol among the protocols available for a client to use in communicating with a server regardless of whether firewalls or proxies exist in the network. This has nothing to do with a stream server apparatus including a second interface which transmits and receives packets to and from another relevant one client apparatus belonging to a third network, different from the first network, via the third network and without passing through the firewall apparatus or the first network, the second interface being connected to a wide area network, as recited in the claims of the present application. Vellanki et al. does not disclose or suggest anything related to these limitations as recited in the claims of the present application. Vellanki et al. is merely directed to automatically detecting a most advantageous protocol for communication via client computer to a server.

17

Moreover, none of the cited references disclose or suggest a stream transport management module which specifies the first interface or the second interface in accordance with a network attribute and a type of a communication protocol of one of the relevant one client apparatus or the another relevant one client apparatus, or where the process module executes a stream data distribution process based on a user datagram protocol (UDP) as the same communication protocol both for the first and second client apparatuses, as recited in the present claims.

Regarding claims 2-8, Applicants submit that these claims are dependent on independent claim 1 and, therefore, are patentable at least for the same reasons noted previously regarding this independent claim. For example, Applicants submit that none of the cited references disclose or suggest where the process module executes a stream data distribution process based on a same communication protocol for both the relevant one of the client apparatuses belonging to the first network and the another relevant one the client apparatuses belonging to the second network different from the first network, or where the stream transport module specifies the first interface if a client apparatus of the client apparatuses belongs to the second network different from the first network for which the firewall apparatus inhibits illegal accesses and if the communication protocol includes a reception process of a packet on a side of the stream server apparatus, or where the stream transport management model specifies the second interface if a client apparatus of the client apparatuses belongs to the second network different from the first network for which the firewall apparatus inhibits illegal accesses and if the communication

protocol does not include a reception process of a packet on a side of the stream server apparatus.

Accordingly, Applicants submit that none of the cited references, taken alone or in any proper combination, disclose, suggest or render obvious the limitations in the combination of each of claims 1-8, 11, 12 and new claim 13 of the present application. Applicants respectfully request that these rejections be withdrawn and that these claims be allowed.

Claim 9 has been rejected under 35 U.S.C. §103(a) as being unpatentable over Vaid et al., Birrell et al. and Vellanki et al. and further in view of Young et al. Applicants respectfully traverse this rejection.

Young et al. discloses methods and systems using a media gateway control protocol (MGCP) application layer gateway for delivery of VoIP packets to Internet protocol phones and to client adapters. The invention provides a customer premises device acting as a proxy between a single Wide Area Network Extranet IP address and any number of MGCP client adapter and MGCP phones.

Applicants submit that claim 9 is dependent on independent claim 1 and, therefore, is patentable at least for the same reasons noted previously regarding this independent claim. Applicants submit that Young et al. does not overcome the substantial defects noted previously regarding Vaid et al., Birrell et al. and Vellanki et al. For example, Applicants submit that none of the cited references disclose or suggest where the control requests reception unit notifies the relevant one and the another relevant one of the client apparatuses of the ID of the specific

interface, the ID being not a local ID distinguishable by the first network for which the firewall apparatus inhibits illegal accesses but a global ID capable of being translated into the local ID by a network relay apparatus en route to a client apparatus requested stream data distribution.

Accordingly, Applicants submit that none of the cited references, taken alone or in any proper combination, disclose, suggest or render obvious the limitations in the combination of claim 9 of the present application. Applicants respectfully request that this rejection be withdrawn and that this claim be allowed.

Claim 10 has been rejected under 35 U.S.C. §103(a) as being unpatentable over Vaid et al., Birrell et al., Vellanki et al. and further in view of Day et al. Applicants respectfully traverse this rejection.

Day et al. discloses a system, method and computer program being provided for a control server in a client/server environment where an API framework facilitates scalable, network transparent, integrated multimedia content loading and data streaming. Concurrent real time content loading and data streaming are possible and techniques are included for admitting new streams only when they can be serviced without negatively affecting current system performance.

Applicants submit that claim 10 is dependent on independent claim 1 and, therefore, is patentable at least for the same reasons noted previously regarding this independent claim. Applicants submit that Day et al. does not overcome the substantial defects noted previously regarding Vaid et al., Birrell et al. and Vellanki et al. For example, Applicants submit that none of the cited references

20

disclose or suggest where the process module includes a stream transport processing unit for executing stream data distribution to the client apparatuses based upon one stream data distribution protocol, and a bandwidth management processing unit for executing bandwidth control communication based on a control program for controlling a bandwidth of the stream data distribution.

Accordingly, Applicants submit that none of the cited references, taken alone or in any proper combination, disclose, suggest or render obvious the limitations in the combination of claim 10 of the present application. Applicants respectfully request that this rejection be withdrawn and that this claim be allowed.

In view of the foregoing amendments and remarks, Applicants submit that claims 1-13 are now in condition for allowance. Accordingly, early allowance of such claims is respectfully requested.

To the extent necessary, Applicants petition for an extension of time under 37 CFR 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to the deposit account of Mattingly, Stanger, Malur & Brundidge, P.C., Deposit Account No. 50-1417 (referencing attorney docket no. 500.43372X00).

Respectfully submitted,

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.

Frederick D. Bailey
Registration No. 42,282

FDB/sdb
(703) 684-1120